



# 2025 NORTH AMERICA COMMUNITY MEETING

# Revolutionizing PCI DSS Assessments with AI



# Jin Chang

CEO & Co-Founder  
Fieldguide



# Phil Del Bello

Head of Solutions  
Fieldguide

# Agenda

By the end of this session, you'll learn:

- How to align AI with the PCI SSC's 2025 guidance
- Where AI accelerates the real assessment workflow
- QA and transparency practices that keep your firm compliant, credible, and trusted

# PCI SSC Guidance: Guardrails, Not Roadblocks

The PCI Security Standards Council issued its first AI guidance in 2025. Three clear messages came through.

## Efficiency gains are achievable

AI can cut manual effort by automating reviews and work papers, boosting accuracy and consistency.

## Transparency is mandatory

Assessors should clearly disclose where and how AI is used, oversight processes, and obtain explicit client consent before relying on AI in assessments.

## Quality assurance is non-negotiable

All AI-generated work should be carefully validated, reviewed, and documented to ensure it meets the same standards as human-produced evidence.

# The Assessment Burden

50-60% of hours

are eaten up by **document reviews**

Disparate systems

Multiple systems and owners create complexity

Sampling trouble

Inconsistent practices lead to errors

Repetitive reports

ROC/AoC process is repetitive and manual

The Council knows this creates bottlenecks — and this is where AI, responsibly applied, shines.

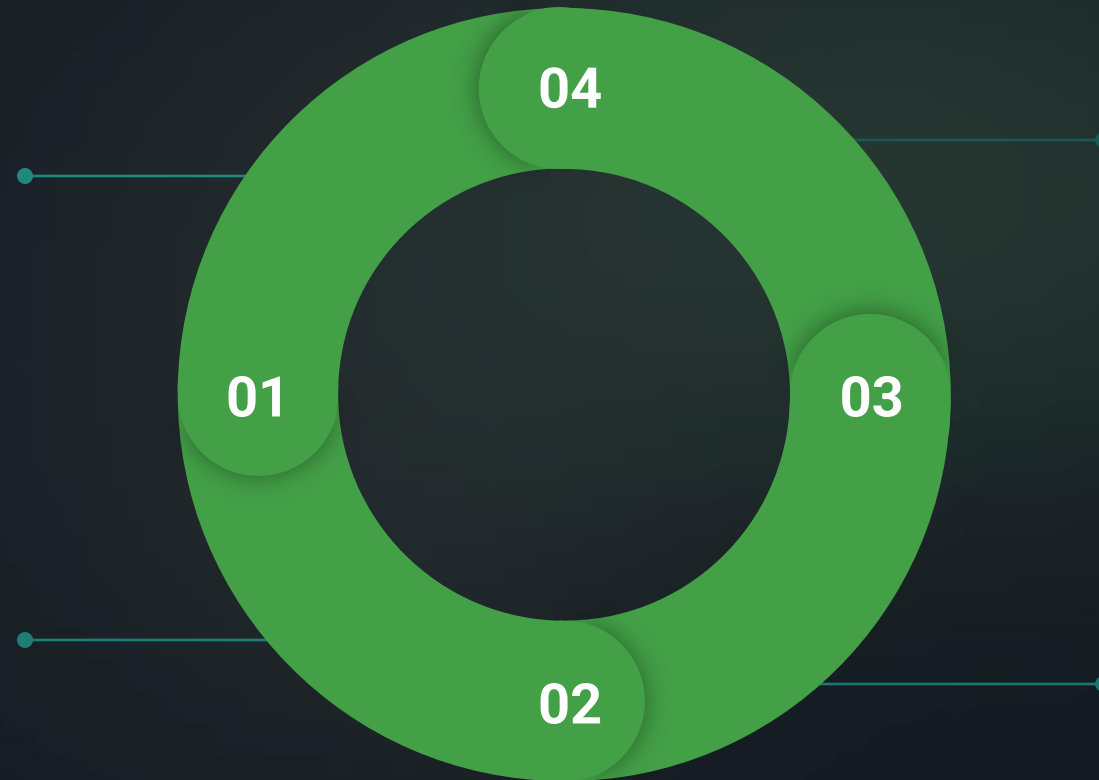
# AI Across the PCI Workflow

## Interviews

- ✓ Consolidate and summarize transcripts into concise "Brief Descriptions" for the ROC.
- ✓ **Tag each statement to the relevant PCI requirement.**
- ✓ **Create action-item lists for follow-up.**

## Documentation & Evidence Review

- ✓ Pull out relevant clauses, configurations, or data.
- ✓ Parse through hundreds of files to identify compliance issues that might take a human assessor days to uncover.
- ✓ Highlight gaps or inconsistencies across multiple sources.



## Quality Assurance

- ✓ Do workpapers and assessor descriptions match findings?
- ✓ Do ROC descriptions align with evidence and client scope?
- ✓ Are any compensating controls undocumented?

## Sampling

- ✓ Compare a client's data sets to the predefined sample list.
- ✓ Automatically flag where items are missing, duplicated, or inconsistent across entire populations and logs of data.
- ✓ Present the assessor with a clean, validated sample set ready for testing.

# AI in Practice - How to select the right platform

## AI Chat Tools

- Generic for broad use
- Risky if used ad hoc

## Purpose-built Agentic Platforms

- Designed for assessors
- Perform multi-step tasks

## Privacy by Design

- Client data is never used to train models

## Aligned with SSC Guidance

- Assessors accountable

*Takeaway: Future-proof firms don't just "bolt on" chat AI. They adopt integrated, assessment-aware AI platforms that streamline compliance while meeting the Council's standards for accountability, transparency, and quality.*

# Guardrails: Keeping AI Compliant

## Oversight

- ✓ The lead assessor owns all conclusions.
- ✓ AI outputs are drafts only.

## Transparency

- ✓ Disclose AI usage in plain English.
- ✓ Gain client consent upfront.

## QA

- ✓ Cross-check AI outputs with raw evidence.
- ✓ Peer review findings.
- ✓ Use QA reviewers with independence.

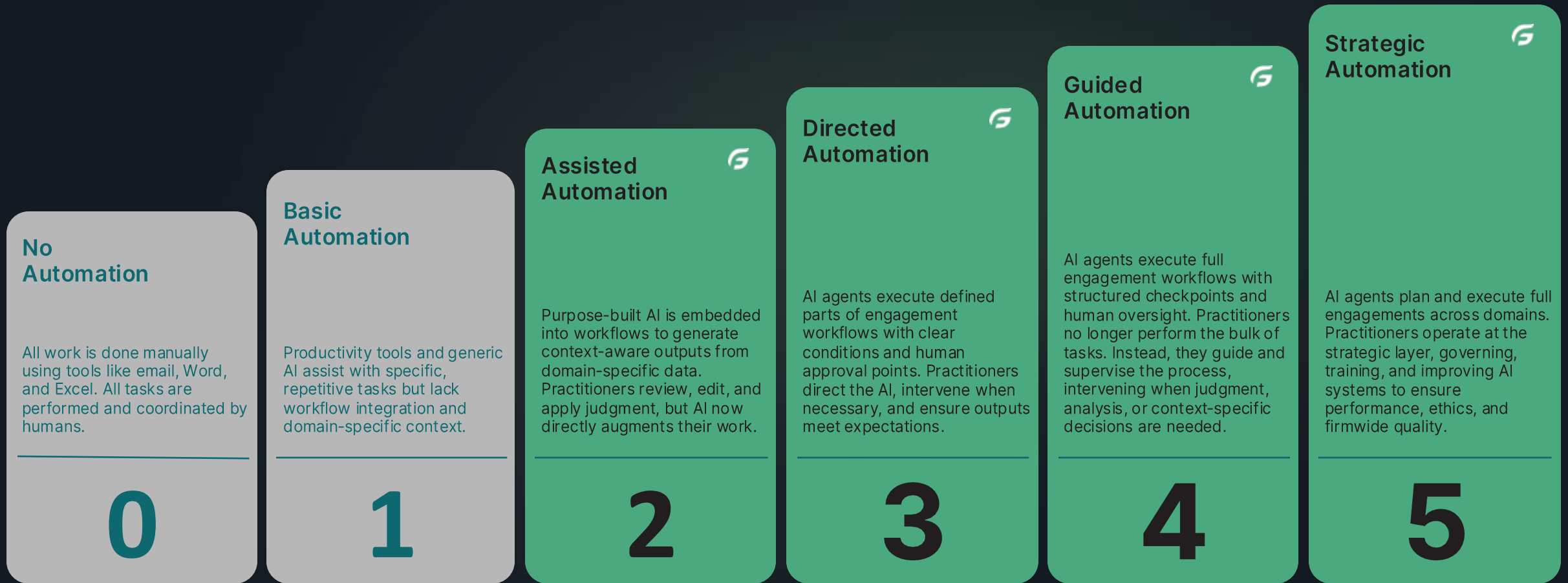
# Documented Policies & Procedures for AI Use

What should be included in your internal AI Use Policies and Procedures?

- Define AI's Role
- Set Standards for Accuracy
- Define Qualification Requirements
- Control Evidence Handling
- Protect Client Data
- Keep Policies Current

*Takeaway: Written policies make AI use clear, transparent, and defensible — for assessors, clients, and regulators alike.*

# AI Maturity Framework: Powering The Firm of the Future



Agentic AI

# Key Takeaways

- AI aligns with SSC guidance if assessors remain responsible.
- Efficiency gains are real: interviews, evidence review, sampling, and QA all accelerate.
- Quality matters most: cross-checks, peer review, and transparency keep trust intact.



# 2025 NORTH AMERICA COMMUNITY MEETING